UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,550	06/30/2003	Ben Smith	0026-0027	7373

44989 7590 11/05/2008
HARRITY & HARRITY, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
NOORISTANY, SULAIMAN	

ART UNIT	PAPER NUMBER
2446	

MAIL DATE	DELIVERY MODE
11/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/608,550	SMITH ET AL.	
	Examiner	Art Unit	
	SULAIMAN NOORISTANY	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/30/3003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

This Office Action is response to the application (10/608550) filed on 25 September 2008.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114. including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 7 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/18/08 has been entered.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-2, 4-11, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stuart** U.S. Patent No**. US 6661431** in view of **Messer US** U.S. Patent No. **7020622.**

Regarding claim 1, Stuart teaches wherein, a system for detecting click spam at a web site, comprising:

collecting information associated with a group of users visiting a web site **(Fig. 1,**

unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67);

identifying non-malicious users visiting the web site from the group of users visiting the web site based on the collected information **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**; and

Determining at least in part on a behavior of the identified non-malicious users **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5 – col. 8, lines 66)**.

However, with respect to claim 1, Stuart is silent in terms of *"an occurrence of spamming on the web site based."*

Messer teaches that it is well known to determine "an occurrence of spamming on the web site based" **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes, artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14)** in order to make the system more efficient and further equipped to deter fraud and other non-productivity activity (col. 4, lines 40-42).

It would have been obvious to one ordinary skill in the art that when the invention was made to modify Stuart's invention by adding a system to includes the ability to track select USER activity while on the Web including interactions with Web pages and click-through navigation to select Web sites where purchases can be executed. Notwithstanding these advancements and advantages, commerce on the web can still

be improved upon. Recognizing some of the current difficulties in implementing affiliate programs has led to the innovations presented herein, as taught by Messer (col. 1, lines 40-50).

Regarding claim 2, Stuart and Messer together taught the method as in claim 1 above. Stuart further teaches wherein the collecting information includes: tracking activities of the group of users visiting the web site **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests, and may track how long each visitor remains on each page – col. 5, lines 35-37).**

Regarding claim 4, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: determining whether the users in the group of users have JavaScript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**.

Regarding claim 5, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: determining a type of

browser used by the users in the group of users **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16**).

Regarding claim 6, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: determining an interval at which each of the users in the group of users visits the web site **(time interval – col. 6, lies 16-17)**.

Regarding claim 7, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein the web site is a search engine **(search engine – col. 5, lines 26-27)**, and wherein the tracking activities includes: determining a type of items for which searches are performed by the users in the group of users **(Transaction Tracking – col. 1, lines 20-36)**.

Regarding claim 8, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: tracking activities of users in the group of users visiting another web site **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16**).

Regarding claim 9, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein each of the users in the group of users is associated with a cookie identifier, and wherein the tracking includes: using the cookie identifiers to

track the activities of the users in the group of users **(During the linking process, the USER has an identifier string appended to the HTTP entry, and possibly a "cookie" placed on their system. These act as a marker to permit tracking of the USER by the Clearinghouse, to determine if and when the USER was involved in a purchase – col. 4, lines 5-11)**.

Regarding claim 10, Stuart and Messer together taught the method as in claim 1 above. Messer further teaches wherein each of the users in the group of users is associated with a cookie identifier, and wherein the identifying non-malicious users includes:

identifying non-malicious users based at least in part on an age of the cookie identifiers associated with the users in the group of users **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2, lines 15-20)**.

Regarding claim 11, Stuart and Messer together taught the method as in claim 1 above. Stuart further teaches wherein each of the users in the group of users is associated with a network address, and wherein the identifying non-malicious users includes:

identifying the non-malicious users based at least in part on the network addresses associated with the users in the group of users **(Fig. 4 -- visitors are identified, preferably by his or her IP, domain or URL address, or any combination thereof – col. 11, lines 31-33)**.

Regarding claim 16, Stuart teaches wherein, a system for detecting click spam at a web site, comprising:

collecting information associated with a group of users visiting a web site **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**;

identifying non-malicious users visiting the web site from the group of users visiting the web site based on the collected information **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**; and

Determining at least in part on a behavior of the identified non-malicious users **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5 – col. 8, lines 66)**.

However, with respect to claim 1, Stuart is silent in terms of *"an occurrence of spamming on the web site based."*

Messer teaches that it is well known to determine "an occurrence of spamming on the web site based" **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes,**

artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14) in order to make the system more efficient and further equipped to deter fraud and other non-productivity activity (col. 4, lines 40-42).

It would have been obvious to one ordinary skill in the art that when the invention was made to modify Stuart's invention by adding a system to includes the ability to track select USER activity while on the Web including interactions with Web pages and click-through navigation to select Web sites where purchases can be executed. Notwithstanding these advancements and advantages, commerce on the web can still be improved upon. Recognizing some of the current difficulties in implementing affiliate programs has led to the innovations presented herein, as taught by Messer (col. 1, lines 40-50).

Claim 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stuart** U.S. Patent No. **US 6661431** in view of **Messer** US U.S. Patent No**. 7020622** further in view of **Srinivasan** U.S. Patent App. Publication No. **US 2002/0042738.**

Regarding claim 12, Stuart and Messer together taught the method as in claim 1 above. Stuart further teaches wherein the web site includes at least one advertisement **(a product advertised on the web page – col. 7, lines 60-61),**

However, Stuart and Messer both are silent in terms of "*determining a click rate of the at least one advertisement for the identified non-malicious users, and*

determining that the at least one advertisement has been spammed when the

click rate of users visiting the web site exceeds the determined click rate for the identified non-malicious users"

Srinivasan further teaches that it is well known to determining a click rate of the at least one advertisement for the identified non-malicious users **(TABLE. 1 illustrates the results of the first iteration of an experiment conducted using the inventive system – [0016])**, and

determining that the at least one advertisement has been spammed when the click rate of users visiting the web site exceeds the determined click rate for the identified non-malicious users **(the minimum effectiveness threshold is 1% --TABLE. 1, illustrates the results of the first iteration of an experiment conducted using the inventive system – [0016]).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Stuart's invention by method and system of the present invention, which enables Internet businesses to conduct real-time, online experiments on a sample of transactions to determine marketplace sensitivities. In addition, it is also common for websites to closely monitor "click-through." Click-through is the number of times users arrive at a site by having clicked on an advertisement. This information is utilized to learn how well an advertisement draws an audience. In view of the foregoing, it can be appreciated that a substantial need exists for a method and system for dynamically determining the effectiveness of various advertisements, as taught by Srinivasan [0023-0024].

Claim 13-14, 17-21, 23-30, 33-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stuart** U.S. Patent No. **US 6661431** in view of **Messer** US U.S. Patent No. **7020622** further in view of **Srinivasan** U.S. Patent App. Publication No. **US 2002/0042738** further in view of **Mason** U.S. App. Publication No. **US 2022/0161648.**

Regarding claim 13, Stuart, Messer and Srinivasan together taught the method as in claim 12 above. However, Stuart, Messer and Srinivasan are silent in terms of "*wherein, the click rate includes a range of click rates*"

Mason further teaches that it is well known to assign wherein, the click rate includes a range of click rates **(the soup company could purchase a million hits on one or a number of URLs or 15,000 click-throughs from one or a plurality of URLs – [0024])**.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Stuart's invention by monitoring the number of click-throughs on each of the ads, a more successful derivative advertisement link, i.e., one which receives a greater number of click-through, can be substituted for the less successful banners, as taught by Mason.

Regarding claim 14, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Stuart further teaches wherein the web site includes at least one advertisement **(a product advertised on the web page – col. 7, lines 60-61)**

wherein the identifying includes:

determining a percentage of users in the group of users visiting the web site in a time period that are non-malicious users **(It is estimated that the website receives 100,000 visitors a day – [0114])**, and

Mason further teaches wherein determining an occurrence of spamming includes:

estimating a percentage of non-malicious users selecting the at least one advertisement during the time period to be approximately the percentage of non-malicious users visiting the web site during the time period **(if it is found that a soup advertisement is receiving more click-throughs in the late afternoon and ads for a financial services firm are receiving more click-throughs early in the morning, then the placement of those particular ads can be modified in order to maximize the number of click-throughs for the advertisers – [0029])**

Srinivasan further teaches wherein determining that the at least one advertisement has been spammed when an actual percentage of non-malicious users selecting the at least one advertisement during the time period is lower than the estimated percentage of non-malicious users selecting the at least one advertisement during the time period **(the minimum effectiveness threshold is 1% --TABLE. 1, illustrates the results of the first iteration of an experiment conducted using the inventive system – [0016]).**

Regarding claims 17, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason also teach a computer-readable medium containing instructions for controlling at least one processor to perform a method for detecting click spamming of an advertisement on a server, the method comprising:

Srinivasan teaches wherein determining a number of non-malicious users accessing the server **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049])**

determining a percentage of the non-malicious users clicking the advertisement when the advertisement is displayed to the non-malicious users **(TABLE. 1 -- [0016])**; and

determining whether the advertisement has been click spammed based at least in part on the determined percentage **(if the measured effectiveness of an advertisement does not meet a minimum threshold, it is deleted from the advertisements -- [0112], Page. 7, TABLE. 1).**

Mason further teaches wherein determining a percentage of the non-malicious users clicking the advertisement when the advertisement is displayed to the non-malicious users; and determining whether the advertisement has been click spammed based at least in part on the determined percentage **(if the derivative advertisement links from one original ad are receiving 20% more click-throughs than the derivative advertisement links created from a second original ad, then some or all**

of the placements of the second original ad can be automatically replaced by the more successful ad -- [0029]).

Regarding claim 18, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason also teach a server comprising:

Mason teaches wherein a memory configured to store at least one advertisement **(memory of computing device -- [0015])**; and

A processor configured to **(a central processor -- [0016)**:

Cause the at least one advertisement to be displayed **(displayed on a computer screen -- [0016])**,

Mason further teaches wherein determining a percentage of the non-malicious users clicking the advertisement when the advertisement is displayed to the non-malicious users; and determining whether the advertisement has been click spammed based at least in part on the determined percentage **(if the derivative advertisement links from one original ad are receiving 20% more click-throughs than the derivative advertisement links created from a second original ad, then some or all of the placements of the second original ad can be automatically replaced by the more successful ad -- [0029]).**

Srinivasan further teaches wherein determining a number of non-malicious users accessing the server **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049])**

determining a percentage of the non-malicious users clicking the advertisement when the advertisement is displayed to the non-malicious users **(the minimum effectiveness threshold is 1% -- [0114])**; and

determining whether at least one the advertisement has been click spammed based at least in part on the determined percentage **(if the measured effectiveness of an advertisement does not meet a minimum threshold, it is deleted from the advertisements -- [0112], TABLE. 1 -- [0016]).**

Regarding claim 19, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason also teach a method for determining whether an item on a web site has been click spammed, comprising:

Srinivasan teaches wherein identifying a group of non-malicious users visiting the web site **(the population may include every potential customer that visits the website. Alternatively, the population may be clustered or segmented, and only visitors that meet a certain profile are considered to be within the population -- [0100])**

determining a click rate of an item associated with the website for the group of non-malicious users **(100,000. , click-through rate threshold -- [0114])**

determining whether the item has been click spammed based at least in part on the determined click rate for the non-malicious users **(the minimum effectiveness threshold is 1% was determined -- [0114], see Page. 7, Table. 1).**

Regarding claim 20, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Mason further teaches wherein, determining a total number of users visiting the web site, and wherein the determining whether the item has been click spammed includes:

comparing the determined click rate for the non-malicious users to a click rate for the total number of users visiting the web site **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**, and

Srinivasan further teaches wherein, determining a total number of users visiting the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);**

determining that the item has been click spammed when the click rate for the total number of users exceeds the determined click rate for the non-malicious users **(the click-through rate, and the effectiveness threshold is 1% -- [0114] "Note: the**

threshold value determines whether the ad has been spammed or not").

Regarding claim 21, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein the identifying includes:

tracking an activity of users visiting the web site (**information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0048]**), and

Mason further teaches wherein tracking an activity of users visiting the web site and identifying the group of non-malicious users based at least in part on the tracked **(monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**.

Regarding claim 23, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein, taking remedial measures in response to determining that the item has been click spammed **([0039] -- FIG. 4 is a flowchart illustrating the process used to measure Internet advertising effectiveness by the method and system of the present invention).**

Regarding claim 24, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein, the determining a click rate of the item for the group of non-malicious users includes:

estimating a percentage of non-malicious users visiting the web site **(It is estimated in this example that the website receives 100,000 visitors a day -- [0114])**, and setting a percentage of clicks of the item from non-malicious users to approximately equal the estimated percentage **(the minimum effectiveness threshold is 1%-- [0114]).**

Regarding claim 25, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein the determining whether the item has been click spammed includes:

determining whether an actual click rate of the item for the group of non-malicious users differs from the set percentage of clicks of the item **(The statistics typically include, the number of visitors who actually click-through each advertisement – [0084] and also the percentage of visitors to a website that not only click-through the advertisement, but actually buy the advertised product – [0086])**.

Regarding claim 26, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Mason further teaches wherein the determining a click rate of the item includes:

determining different click rates of the item for the group of non-malicious users, the different click rates corresponding to different time periods **(time period –[0022])**.

Regarding claim 27, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Mason further teaches wherein the different time periods include different times of a day or week **(short time period – [0022] "Note: short time period can be any time of a day and or any day of a week)**.

Regarding claim 28, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above. Mason further teaches wherein, the different time periods include different months of a year **(short time period – [0022] "Note: short time period can be any month of a year).**

Regarding claim 29, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason also teach a computer-readable medium containing instructions for controlling at least one processor to perform a method for detecting a spamming of an advertisement displayed by a server, as described above. The method comprising:

Srinivasan teaches wherein identifying non-malicious users visiting the web site **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049])**

determining a click rate of the item for the group of non-malicious users **(the click-through rate and the threshold percentage 1% -- [0114])**

determining whether the item has been click spammed based at least in part on the determined click rate for the non-malicious visitors **(the minimum effectiveness threshold is 1% was determined -- [0114], see Page. 7, Table. 1).**

Regarding claim 30, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason also teach a server comprising:

Mason teaches wherein a memory configured to store at least one advertisement **(memory of computing device -- [0015])**; and

A processor configured to **(a central processor -- [0016])**:

Cause the at least one advertisement **(ad or banner)** to be displayed **(displayed on a computer screen -- [0016])**,

Identify a number non-malicious users accessing the server **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049])**

compare the number of non-malicious users to a total number of users to obtain a percentage **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in**

order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022]),

Srinivasan further teaches wherein set a click rate of the at least one item based at least in part on the percentage **(maximize the click-through rate, and the minimum effectiveness threshold is 1% -- [0114])**, and

determine whether the at least one item has been spammed based at least in part on the click rate **(if the measured effectiveness of an advertisement does not meet a minimum threshold, it is deleted from the advertisements -- [0112], TABLE. 1 – [0016]).**

Regarding claim 33, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 16 above where the means for tracking at least one activity of the identified non-malicious visitors includes at least one of:

Srinivasan further teaches means for determining a percentage of visitors in a group of visitors visiting the web site in a time period that are non-malicious visitors (**percentage of visitors to a website – [0086]**), and where the means for determining an occurrence of click spamming includes:

means for estimating a percentage of non-malicious visitors selecting an advertisement associated with the web site during the time period to be approximately

the percentage of non-malicious visitors visiting the web site during the time period **(It is estimated in this example that the website receives 100,000 visitors a day -- [0114])**, and

means for determining that the advertisement has been spammed when an actual percentage of non-malicious visitors selecting the advertisement during the time period is lower than the estimated percentage of non-malicious visitors selecting the advertisement during the time period **([0039] -- FIG. 4 is a flowchart illustrating the process used to measure Internet advertising effectiveness by the method and system of the present invention).**

Regarding claim 34, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 17 above. Mason further teaches wherein the determining whether the advertisement has been click spammed based at least in part on the determined percentage includes:

comparing the determined percentage of the non-malicious users clicking the advertisement to a percentage of non-malicious users clicking the advertisement from a different time period **((the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a**

particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022]).

Regarding claim 35, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 17 above. Mason further teaches where the determining whether the advertisement has been click spammed includes:

estimating a percentage of non-malicious users clicking the advertisement to be approximately a percentage of non-malicious users accessing the server **(if it is found that a soup advertisement is receiving more click-throughs in the late afternoon and ads for a financial services firm are receiving more click-throughs early in the morning, then the placement of those particular ads can be modified in order to maximize the number of click-throughs for the advertisers – [0029])**, and

Srinivasan further teaches determining that the advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the advertisement is lower than the estimated percentage of non-malicious users clicking the advertisement **(the minimum effectiveness threshold is 1% --TABLE. 1, illustrates the results of the first iteration of an experiment conducted using the inventive system – [0016]).**

Regarding claim 36, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 18 above, mason further teaches wherein when determining whether the at

least one advertisement has been click spammed, the processor is configured to: compare the determined percentage of the non-malicious users clicking the at least one advertisement to a percentage of non-malicious users clicking the at least one advertisement from a different time period **(if the derivative advertisement links from one original ad are receiving 20% more click-throughs than the derivative advertisement links created from a second original ad, then some or all of the placements of the second original ad can be automatically replaced by the more successful ad -- [0029]).**

Regarding claim 37, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 18 above, Srinivasan further teaches wherein when determining whether the at least one advertisement has been click spammed, the processor is configured to:

estimate a percentage of non-malicious users clicking the at least one advertisement to be approximately a percentage of non-malicious users visiting the server (**percentage of visitors to a website – [0086]**), and

determining that the at least one advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the at least one advertisement is lower than the estimated percentage of non-malicious users clicking the at least one advertisement **([0039] -- FIG. 4 is a flowchart illustrating the process used to measure Internet advertising effectiveness by the method and system of the present invention).**

Regarding claim 38, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 19 above, Mason further teaches wherein where the method further comprises:

determining a total number of visitors to the server, and

where the determining whether the advertisement has been spammed includes: (**the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**, and

Srinivasan further teaches wherein, determining a total number of users visiting the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);** determining that the item has been click spammed when the click rate for the total number of users exceeds the determined click rate for the non-malicious users **(the click-through rate, and the effectiveness threshold is 1% -- [0114] "Note: the threshold value determines whether the ad has been spammed or not").**

Claims 3, 15, 22, 31-32 39-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stuart** U.S. Patent No. **US 6661431** in view of **Messer** US U.S. Patent No**. 7020622** further in view of **Srinivasan** U.S. Patent App. Publication No. **US 2002/0042738** further in view of **Mason** U.S. App. Publication No. **US 2022/0161648** further in view of **Ishikawa** Patent App. Publication No **US US. 2001/0037314.**

Regarding claims 31, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 13 above. Therefore, Stuart, Messer, Srinivasan and Mason further teach a method including:

Stuart further teaches tracking activities of users visiting a web site, the tracking including determining **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests, and may track how long each visitor remains on each page – col. 5, lines 35-37),** identifying non-malicious users from among the users visiting the web site based at least in part on the tracked activities **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67),**

Messer further teaches an age of a cookie associated with each user **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2,**

lines 15-20), whether the user has javascript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**, a type of browser used by the user **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**, or an interval at which the user visits the web site **(time interval – col. 6, lies 16-17).** Stuart, Messer, Srinivasan and Mason are silent in terms "*loading image*".

However, Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Further it would have been obvious to one ordinary skilled in the art in the time the invention was made to combine the teaching of Ishikawa for loading images onto the user's devices, which will provide a generated confirmation code.

Motivation would be to provide a true recognition of the users devices as suggested by Ishikawa for comparing the users information to aspects of the confirmation code, namely, the user identification at the time the advertisement link is loaded onto the user's computer.

Regarding claim 3, it has the similar limitation as of claim 31; therefore, it's rejected under the same rationale as in claim 31.

Regarding claim 15, Ishikawa further teaches providing a refund in response to determining that the at least one advertisement has been spammed **(Once the information is recorded in the advertiser's log, the entry is further passed to an accounting management system, which tracks the amount of *remuneration* owed to each advertiser, this procedure take place while the click is not spam [0052])**.

Regarding claim 22, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 31 above. Therefore, Stuart, Messer, Srinivasan and Mason further teach a method including:

Stuart further teaches tracking activities of users visiting a web site, the tracking including determining **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests, and may track how long each visitor remains on each page – col. 5, lines 35-37),** identifying non-malicious users from among the users visiting the web site based at least in part on the tracked activities **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**,

Messer further teaches an age of a cookie associated with each user **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2,**

lines 15-20), whether the user has javascript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**, a type of browser used by the user **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**, or an interval at which the user visits the web site **(time interval – col. 6, lies 16-17)**

Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Regarding claim 32, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 31 above. Therefore, Stuart, Messer, Srinivasan and Mason further teach a method including:

Stuart further teaches tracking activities of users visiting a web site, the tracking including determining **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests, and may track how long each visitor remains on each page – col. 5, lines 35-37),** identifying non-malicious users from among the users visiting the web site based at least in part on the tracked activities **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**,

Messer further teaches an age of a cookie associated with each user **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2, lines 15-20)**, whether the user has javascript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**, a type of browser used by the user **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**, or an interval at which the user visits the web site **(time interval – col. 6, lies 16-17)**

Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Regarding claim 39, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 31 above. Therefore, Stuart, Messer, Srinivasan and Mason further teach a method including:

Stuart further teaches tracking activities of users visiting a web site, the tracking including determining **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests,**

and may track how long each visitor remains on each page – col. 5, lines 35-37), identifying non-malicious users from among the users visiting the web site based at least in part on the tracked activities **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67)**,

Messer further teaches an age of a cookie associated with each user **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2, lines 15-20)**, whether the user has javascript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**, a type of browser used by the user **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**, or an interval at which the user visits the web site **(time interval – col. 6, lies 16-17)**

Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Regarding claim 40, Stuart, Messer, Srinivasan and Mason together taught the method as in claim 31 above. Therefore, Stuart, Messer, Srinivasan and Mason further teach a method including:

Stuart further teaches tracking activities of users visiting a web site, the tracking including determining **(The method collects data regarding a visitor's navigation between web pages, and tracks how long the visitor remains on each page – col. 4, lines 53-55; data may be collected regarding which pages each visitor requests, and may track how long each visitor remains on each page – col. 5, lines 35-37),** identifying non-malicious users from among the users visiting the web site based at least in part on the tracked activities **(Fig. 1, unit 12 – identify and collect information pertaining to entities; unit 14 – collect navigation information – col. 7, lines 5-67),**

Messer further teaches an age of a cookie associated with each user **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2, lines 15-20)**, whether the user has javascript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**, a type of browser used by the user **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**, or an interval at which the user visits the web site **(time interval – col. 6, lies 16-17)**

Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Regarding claim 41, Stuart, Messer, Srinivasan, Mason and Ishikawa together taught the method as in claim 31 above. Stuart further teaches wherein where the at least one item includes an advertisement **(a product advertised on the web page – col. 7, lines 60-61).**

Regarding claim 42, Stuart, Messer, Srinivasan, Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein:

determining a quantity of the identified non-malicious users that clicks an advertisement associated with the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);** and

determining whether the advertisement has been spammed based on the determined quantity of the identified non-malicious users that clicks the advertisement **(the click-through rate, and the effectiveness threshold is 1% -- [0114] "Note: the threshold value determines whether the ad has been spammed or not").**

Mason further teaches "determined click rate for the non-malicious users to a click rate for the total number of users visiting the web site" **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential**

fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])

Regarding claim 43, Stuart, Messer, Srinivasan, Mason and Ishikawa together taught the method as in claim 31 above. Messer further teaches wherein determining that spamming occurs on the web site based on a behavior of the non-malicious users visiting the web site **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes, artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14)**.

Response to Amendment

Applicant's arguments with respect to claim(s) 1-43 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can non-maliciously be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu, can be reached on (571) 272-6798. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sulaiman Nooristany 10/29/2008

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446